CONTENTS REPRODUCING DEVICE

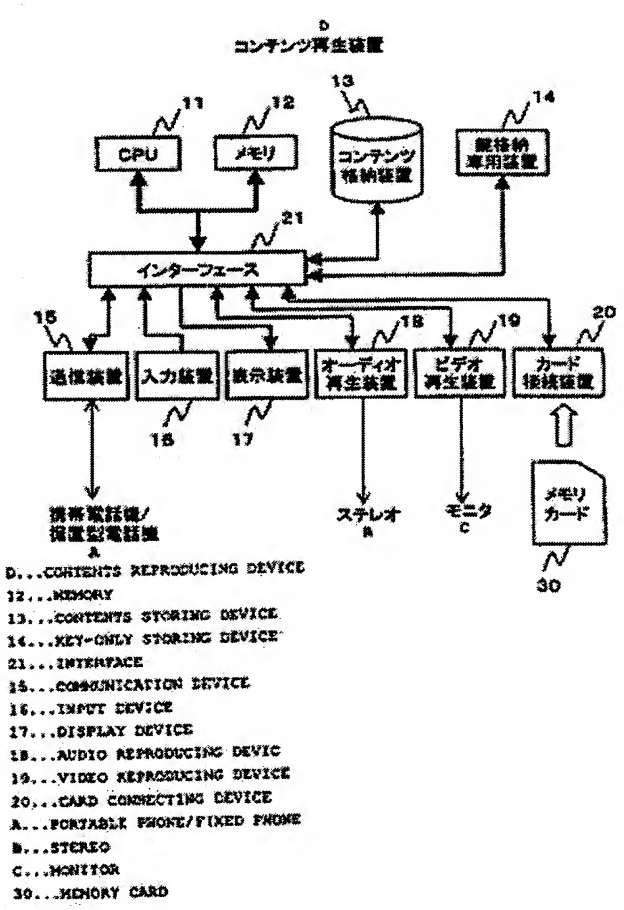
Publication number: WO0169842 (A1)
Publication date: 2001-09-20
Inventor(s): TSUNEHIRO TAKASHI [JP]; KATAYAMA KUNIHIRO [JP]; MIZUSHIMA NAGAMASA [JP]; TOTSUKA TAKASHI [JP]; MANO HIROYUKI [JP]; NAKAMURA KAZUO [JP]; TODOROKI SHIGEO [JP]; HIOKI TOSHIAKI [JP]; HATAKEYAMA TAKAHISA [JP]
Applicant(s): HITACHI LTD [JP]; NIPPON COLUMBIA [JP]; SANYO ELECTRIC CO [JP]; FUJITSU LTD [JP]; TSUNEHIRO TAKASHI [JP]; KATAYAMA KUNIHIRO [JP]; MIZUSHIMA NAGAMASA [JP]; TOTSUKA TAKASHI [JP]; MANO HIROYUKI [JP]; NAKAMURA KAZUO [JP]; TODOROKI SHIGEO [JP]; HIOKI TOSHIAKI [JP]; HATAKEYAMA TAKAHISA [JP]
Classification:
- international: ***G11B20/00; H04L9/10;*** **G11B20/00; H04L9/10;** (IPC1-7): H04L9/08; H04L9/10; H04L9/32
- European: G11B20/00P
Application number: WO2001JP02003 20010314
Priority number(s): JP20000070672 20000314

Also published as:
TW515950 (B)
AU4113101 (A)

Cited documents:
JP9307543 (A)
JP4102185 (A)
JP10040172 (A)
XP002942131 (A)
XP002942132 (A)

Abstract of **WO 0169842 (A1)**

A license key provided for each element of contents data is stored in a key-only storing device provided separately from a contents storing device; the key-only storing device performs an authentication processing on a communicating partner, and, when authenticated, sends a license key corresponding to contents data to be reproduced to a reproducing device using an encrypted communication, whereby the reproducing device decodes the contents data to be reproduced using the license key and reproduces it.



(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年9 月20 日 (20.09.2001)

PCT

(10) 国際公開番号
WO 01/69842 A1

(51) 国際特許分類[7]: H04L 9/08, 9/10, 9/32

(21) 国際出願番号: PCT/JP01/02003

(22) 国際出願日: 2001 年3 月14 日 (14.03.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-70672 2000 年3 月14 日 (14.03.2000) JP

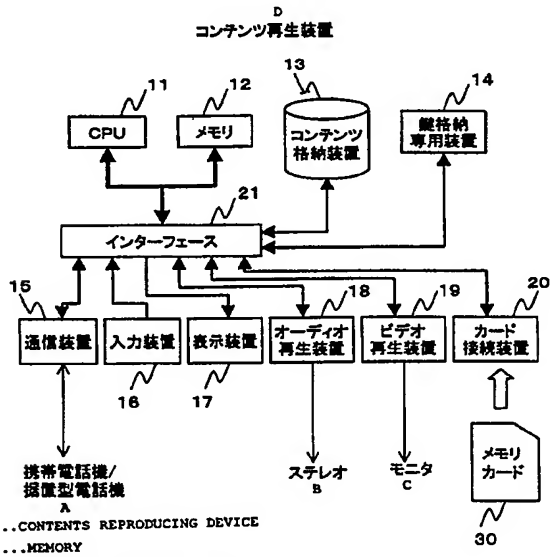
(71) 出願人 (米国を除く全ての指定国について): 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒100-8220 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-0052 東京都港区赤坂4丁目14番14号 Tokyo (JP). 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 常広 隆司 (TSUNEHIRO, Takashi) [JP/JP]. 片山 国弘 (KATAYAMA, Kunihiro) [JP/JP]. 水島 永雅 (MIZUSHIMA, Nagamasa) [JP/JP]. 真野宏之 (MANO, Hiroyuki) [JP/JP]; 〒215-0013 神奈川県川崎市麻生区王禅寺1099番地 株式会社 日立製作所 システム

[続葉有]

(54) Title: CONTENTS REPRODUCING DEVICE

(54) 発明の名称: コンテンツ再生装置



D...CONTENTS REPRODUCING DEVICE
12...MEMORY
13...CONTENTS STORING DEVICE
14...KEY-ONLY STORING DEVICE
21...INTERFACE
15...COMMUNICATION DEVICE
16...INPUT DEVICE
17...DISPLAY DEVICE
18...AUDIO REPRODUCING DEVIC
19...VIDEO REPRODUCING DEVICE
20...CARD CONNECTING DEVICE
A...PORTABLE PHONE/FIXED PHONE
B...STEREO
C...MONITOR
30...MEMORY CARD

(57) Abstract: A license key provided for each element of contents data is stored in a key-only storing device provided separately from a contents storing device; the key-only storing device performs an authentication processing on a communicating partner, and, when authenticated, sends a license key corresponding to contents data to be reproduced to a reproducing device using an encrypted communication, whereby the reproducing device decodes the contents data to be reproduced using the license key and reproduces it.

[続葉有]

WO 01/69842 A1

開発研究所内 Kanagawa (JP). 戸塚 隆 (TOTSUKA, Takashi) [JP/JP]. 中村一男 (NAKAMURA, Kazuo) [JP/JP]; 〒187-0022 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 轟 茂夫 (TODOROKI, Shigeo) [JP/JP]; 〒107-0052 東京都港区赤坂4丁目14番14号 日本コロムビア株式会社内 Tokyo (JP). 日置敏昭 (HIOKI, Toshiaki) [JP/JP]; 〒503-0116 岐阜県安八郡安八町大森180 三洋電機株式会社内 Gifu (JP). 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 富田和子(TOMITA, Kazuko); 〒220-0004 神奈川県横浜市西区北幸二丁目9-10 横浜HSビル7階 Kanagawa (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

コンテンツデータ毎に用意されたライセンス鍵をコンテンツ格納装置とは別に設けられた鍵格納専用装置に格納し、該鍵格納専用装置は通信相手に認証処理を施し、認証された場合には、暗号通信を利用して再生装置に再生対象コンテンツデータに対応するライセンス鍵を送信することで、前記再生装置は再生対象コンテンツデータを、前記ライセンス鍵を用いて復号して再生する。

明細書

コンテンツ再生装置

技術分野

本発明は、正当な権利者のみに、オーディオデータやビデオデータなどのコンテンツデータの再生を許可する技術に関し、特に、大量のコンテンツデータを再生可能な据置型のコンテンツ再生装置に好適な技術に関する。

背景技術

近年、オーディオデータやビデオデータなどのコンテンツデータをネットワークを介して配信しようとする試みがなされている。たとえば、専用のメモリカードを用意し、これを販売店などに設置された専用端末に装着し、オンラインシステムを利用して所望のコンテンツデータを前記メモリカード内にダウンロードする。あるいは、専用のメモリカードを携帯電話機等の個人向け端末に装着し、インターネットを利用して、コンテンツ配信センタから前記メモリカード内にダウンロードする。コンテンツデータを再生する場合には、コンテンツデータを格納した前記メモリカードを専用の再生装置に装着し、再生する。

発明の開示

さて、上述のような専用のメモリカードと再生装置からなるシステム

において、コンテンツデータは複製が容易であることから、コンテンツデータを格納する専用のメモリカードには、コピー防止機能を設けるなどしてコンテンツ著作者などの保護を図る必要がある。

しかしながら、メモリカードでは、容量に限界があるため、大量のコンテンツデータを保存することができない。ユーザは、現在利用していないコンテンツデータであっても、コレクションとしてとっておきたい場合がある。この場合、メモリカードにコピー防止機能が付加されていると、ユーザは、メモリカードがコンテンツデータで満杯になる都度、新たなメモリカードを購入しなければならず、経済的な負担が大きい。

また、ユーザは、コレクションとしてとっておいたコンテンツデータを再生したい場合、数あるメモリカードの中から再生したいコンテンツデータを記憶したメモリカードを見つけ出し、専用の再生装置に装着しなけらばならない。そして、再生したいコンテンツデータを記憶したメモリカードが変わる都度、再生装置に装着するメモリカードを変更しなければならず手間である。

このような、コピー防止機能が付いたメモリカードと再生装置からなるシステムは、携帯用に適しているが、たとえば、家のなかでコンテンツデータの再生を楽しむような据置型には適していない。

本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、コンテンツ著作者などの保護を図りつつも、メモリカードの交換なしに、大量のコンテンツデータを再生できるようにすることにある。

上記課題を解決するために、本発明のコンテンツ再生装置では、コンテンツデータもしくは当該データのグループ毎に異なる鍵で暗号化されたコンテンツデータを再生する。コンテンツデータもしくは当該データのグループ毎に用意された、暗号化されたコンテンツデータを復号するための鍵は、暗号化されたコンテンツデータを格納するコンテンツ格納

手段とは別個に設けられた計算機能付き格納手段に格納しておく。

ここで、計算機能付き鍵格納手段は、通信相手を認証する認証手段を有し、当該認証手段によりコンテンツ再生装置の再生手段が通信相手として認証された場合に、暗号通信を利用して、再生手段に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信する。また、再生手段は、コンテンツ格納手段から読み出された、再生対象の暗号化されたコンテンツデータを、計算機能付き鍵格納手段より暗号通信を利用して送信された鍵を用いて復号し再生する。

本発明において、コンテンツ格納手段に格納されたコンテンツデータは暗号化されているので、対応する鍵がなければ復号し再生することができない。したがって、コンテンツ格納手段にコピー防止機能といった特別な機能を設ける必要がなくなるため、コンテンツ格納手段として、一般に市販されている大容量のハードディスク装置などを利用できる。このため、大量のコンテンツデータを格納することが可能となる。

また、コンテンツ格納手段に格納されたコンテンツデータを復号するためには対応する鍵が必要となるため、この鍵が計算機能付き鍵格納手段に格納されていなければ、当該コンテンツデータを再生することができない。したがって、正当な権利者（対応する鍵を有する者）のみに、コンテンツデータの再生を許可することができ、コンテンツ著作者などの保護を図ることができる。

さらに、本発明では、暗号化されたコンテンツデータの復号を、コンテンツデータの再生を行う再生手段で行うようにしている。そして、計算機能付き鍵格納手段は、鍵の送信相手が再生手段であることを認証した場合に、当該鍵を暗号通信を利用して前記再生手段に送るようにしている。このようにすることで、鍵が外部に漏れる可能性をより低くすることができ、セキュリティを向上できる。

なお、一般に、暗号化されたコンテンツデータを復号するための鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば、著しく小さい。このため、計算機能付き鍵格納手段として、本コンテンツ再生装置に装着自在に構成された、従来の技術で説明したようなコピー防止機能を備えたメモリカードを用いた場合でも、当該メモリカードに大量のコンテンツデータに対応する鍵を格納することができる。したがって、再生するコンテンツを変えるときにメモリカードを差し替えなければならないといった事態が頻繁に生じるのを防ぐことができる。したがって、家のなかでコンテンツデータの再生を楽しむような据置型に適したコンテンツ再生装置を提供できる。

図面の簡単な説明

図１は、本発明の１実施形態が適用されたコンテンツ再生装置の概略構成を示す図である。

図２は、図１に示す鍵格納専用装置１４の概略構成を示す図である。

図３は、図１に示すオーディオ再生装置１８の概略構成を示す図である。

図４は、図１に示すビデオ再生装置１９の概略構成を示す図である。

図５は、本発明の１実施形態が適用されたコンテンツ再生装置の概観の一例を示す図である。

図６は、本発明の第１実施形態が適用されたコンテンツ再生装置の再生動作を説明するためのフロー図である。

図７は、図６に示すフローにおける鍵格納専用装置１４およびオーディオ再生装置１８/ビデオ再生装置１９間のデータのやり取りの一例を説明するためのシーケンス図である。

図８は、本発明の第１実施形態が適用されたコンテンツ再生装置に接続されたメモリカード３０からライセンス鍵を入手する場合の動作を説明するためのフロー図である。

図９は、図８に示すフローにおける鍵格納専用装置１４およびメモリカード３０間のデータのやり取りの一例を説明するためのシーケンス図である。

図１０は、本発明の１実施形態が適用されたコンテンツ再生装置の鍵格納専用装置１４から本コンテンツ再生装置に接続されたメモリカード３０へライセンス鍵を移動する場合の動作を説明するためのフロー図である。

発明を実施するための最良の形態

以下に、本発明の１実施形態について説明する。

図１は、本発明の１実施形態が適用されたコンテンツ再生装置の概略構成を示す図である。

図１において、ＣＰＵ１１は、本コンテンツ再生装置の各部を統括的に制御する。メモリ１２は、ＲＯＭおよびＲＡＭから構成される。ＲＯＭには、ＣＰＵ１１が本コンテンツ再生装置の各部を統括的に制御するためのプログラムが格納されている。ＲＡＭは、ＣＰＵ１１のワークエリアとして機能する。

コンテンツ格納装置１３は、たとえばハードディスク装置などの大容量記憶装置で構成されており、暗号化されたオーディオデータやビデオデータなどのコンテンツデータがそのコンテンツ名称に対応付けられて格納される。

鍵格納専用装置１４は、コンテンツ毎に用意された、暗号化されたコ

ンテンツデータを復号するための鍵（以下、ライセンス鍵と称する）を格納する。

通信装置１５は、携帯電話機や据置型の電話機に接続し、オンラインシステムやインターネットなどのネットワークを介して、たとえば暗号化されたコンテンツデータやライセンス鍵を配信するコンテンツ配信センタ（不図示）にアクセスし、暗号化されたコンテンツデータやライセンス鍵を入手するのに用いられる。

入力装置１６は、たとえば各種ボタンやタッチパネルで構成され、ユーザからの再生指示やコンテンツデータ、ライセンス鍵の入手指示を受け付ける。

表示装置１７は、たとえば液晶パネルで構成され、コンテンツ格納装置１３に格納されている暗号化されたコンテンツデータのコンテンツ名称のリストを表示したり、再生対象の暗号化されたコンテンツデータのコンテンツ名称を表示したりする。

オーディオ再生装置１８は、コンテンツ格納装置１３のなかから再生対象の暗号化されたオーディオデータを読み出し、これに対応するライセンス鍵を用いて復号し再生して、オーディオ信号を得る。そして、オーディオ信号を本コンテンツ再生装置に接続されたステレオに出力する。ビデオ再生装置１９は、コンテンツ格納装置１３のなかから再生対象の暗号化されたビデオデータを読み出し、これに対応するライセンス鍵を用いて復号し再生して、ビデオ信号を得る。そして、ビデオ信号を本コンテンツ再生装置に接続されたモニタに出力する。

カード接続装置２０は、メモリカード３０を接続し、当該メモリカード３０から暗号化されたコンテンツデータやライセンス鍵を入手したり、当該メモリカード２０へ暗号化されたコンテンツデータやライセンス鍵を送ったりする。

インターフェース２１は、ＣＰＵ１１やメモリ１２と本コンテンツ再生装置を構成する他装置との間のデータ送受を司る。

次に、本コンテンツ再生装置を構成する各装置のうち、鍵格納専用装置１４、オーディオ再生装置１８およびビデオ再生装置１９について、さらに詳細に説明する。

まず、鍵格納専用装置１４について説明する。

図２は、鍵格納専用装置１４の概略構成を示す図である。

図示するように、鍵格納専用装置１４は、ＣＰＵ１４１と、メモリ１４２と、フラッシュメモリ１４３と、インターフェース２１を介して本コンテンツ再生装置の各部とデータ送受を行うためのＩ/Ｏ回路１４４と、を有する。

ＣＰＵ１４１は、鍵格納専用装置１４の各部を統括的に制御する。また、ＣＰＵ１４１は、認証機能と暗復号化機能を有している。メモリ１４２は、ＲＯＭおよびＲＡＭから構成される。ＲＯＭには、ＣＰＵ１４１が鍵格納専用装置１４の各部を統括的に制御するためのプログラムと、認証機能および暗復号化機能を実現するためのプログラムが格納されている。ＲＡＭは、ＣＰＵ１４１のワークエリアとして機能する。フラッシュメモリ１４３には、ライセンス鍵が復号対象コンテンツのコンテンツ名称に対応付けられて格納される。ここで、ライセンス鍵は、セキュリティをより強固にするため、いわゆるタンパ・レジスタント領域（TRM:Tamper Resistant Module）に格納するのがよい。なお、フラッシュメモリ１４３の代わりに、ＦＲＡＭやＥＥＰＲＯＭなどのその他の不揮発性メモリを用いることができる。

図２に示す鍵格納専用装置１４を構成する各部は、たとえば１チップ上につくり込まれるようにしてもよいし、あるいは、複数チップで構成されるようにしてもよい。複数チップで構成する場合は、鍵格納専用装

置１４の外部からチップ間の信号を盗み取られないような工夫を施すことが好ましい。

次に、オーディオ再生装置１８について説明する。

図３は、オーディオ再生装置１８の概略構成を示す図である。

図示するように、オーディオ再生装置１８は、暗復号化回路１８１と、デコーダ回路１８２と、インターフェース２１を介して本コンテンツ再生装置の各部とデータ送受を行うためのＩ/Ｏ回路１８４と、を有する。

暗復号化回路１８１は、鍵格納専用装置１４から再生対象の暗号化されたオーディオデータに対応するライセンス鍵を入手し、この鍵を用いて、コンテンツ格納装置１３から読み出された再生対象の暗号化されたオーディオデータを復号する。デコーダ回路１８２は、暗復号化回路１８１で復号化されたオーディオデータを、必要に応じて伸長し、再生して、オーディオ信号を得る。そして、オーディオ信号をステレオに出力する。

次に、ビデオ再生装置１９について説明する。

図４は、ビデオ再生装置１９の概略構成を示す図である。

図示するように、ビデオ再生装置１９は、暗復号化回路１９１と、デコーダ回路１９２と、フレームバッファ１９３と、インターフェース２１を介して本コンテンツ再生装置の各部とデータ送受を行うためのＩ/Ｏ回路１９４とを有する。

暗復号化回路１９１は、鍵格納専用装置１４から再生対象の暗号化されたビデオデータに対応するライセンス鍵を入手し、この鍵を用いて、コンテンツ格納装置１３から読み出された再生対象の暗号化されたビデオデータを復号する。デコーダ回路１８２は、フレームバッファ１９３を利用して、暗復号化回路１８１で復号化されたビデオデータを、必要に応じて伸長し、再生して、ビデオ信号を得る。そして、ビデオ信号を

モニタに出力する。

次に、本コンテンツ再生装置に装着されて用いられるメモリカード３０について説明する。

メモリカード３０の概略構成は、図２に示す鍵格納専用装置１４と同じである。ただし、メモリカード３０には、ライセンス鍵のみならず、暗号化されたコンテンツデータも格納されるものとする。すなわち、このメモリカード３０は、たとえば販売店などに設置された専用端末に装着されて、ユーザがオンラインシステムを利用して所望の暗号化されたコンテンツデータやそのライセンス鍵を入手したり、あるいは、携帯電話機等の個人向け端末に装着されて、ユーザがインターネットを利用してコンテンツ配信センタから所望の暗号化されたコンテンツデータやそのライセンス鍵を入手したりするのに用いることができるものとする。

ここで、図５に、本実施形態が適用されたコンテンツ再生装置の概観の一例を示す。図示するように、本コンテンツ再生装置は、家庭内でコンテンツを楽しむのに適した据置型の形状をしている。ここで、符号４１は、再生ボタン、停止ボタン、再生コンテンツ選択ボタン、および、コンテンツデータやライセンス鍵をコンテンツ格納装置１３や鍵格納専用装置１４へ書き込んだり、カード接続装置３０に接続されたメモリカード２０へ移動したりするための各種設定ボタンなどで構成される操作パネルである。符号４２は、操作パネル４１と同じ各種ボタンを備えたリモコン５０からの指示を受け付けるための受信部である。符号４３は、表示パネルであり、コンテンツ格納装置１３に格納されているコンテンツデータのコンテンツ名称のリストを表示したり、再生対象の暗号化されたコンテンツデータのコンテンツ名称を表示したりする。そして、符号４４は、メモリカード３０を装着するためのスロットである。なお、図示していないが、本コンテンツ装置の背面には、モニタ５１やステレ

オ５２や携帯電話機５３あるいは電話機を接続するための端子が設けられている。

次に、本実施形態のコンテンツ再生装置の動作について説明する。

まず、コンテンツデータを再生する場合の動作について説明する。

図６は、本実施形態が適用されたコンテンツ再生装置の再生動作を説明するためのフロー図である。このフローは、たとえば、ユーザが入力装置１６を用いて、表示装置１７に表示された、コンテンツ格納装置１３に格納されているコンテンツデータのコンテンツ名称のリストのなかから、再生対象のコンテンツを選択し、再生指示を入力すると開始される。

まず、ＣＰＵ１１は、入力装置１６を介してユーザより受け付けたコンテンツデータの再生指示を、当該コンテンツデータの種類（オーディオデータ/ビデオデータ）を再生するオーディオ再生装置１８/ビデオ再生装置１９に送信する（Ｓ１００１）。

ＣＰＵ１１より再生指示を受け取ったオーディオ再生装置１８/ビデオ再生装置１９の暗複号化回路１８１/１９１は、自身の認証データと再生対象の暗号化されたコンテンツデータの識別情報（たとえばコンテンツ名称）を含んだ、当該コンテンツデータ再生のためのライセンス鍵送信指示を、鍵格納専用装置１４に送信する（Ｓ１００２）。

鍵格納専用装置１４のＣＰＵ１４１は、コンテンツデータ再生のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う（Ｓ１００３）。たとえば、認証データが予め本鍵格納専用装置１４に登録されているオーディオ/ビデオ再生装置であることを示しているか否かを調べる。そして、当該指示の送信元がオーディオ再生装置１８/ビデオ再生装置１９であることを認証したならば（Ｓ１００４でＹｅｓの場合）、当該指示に含まれる識別情報によ

り特定されるコンテンツデータのライセンス鍵がフラッシュメモリ１４３に格納されているか否かを調べる（Ｓ１００５）。格納されていれば（Ｓ１００６でＹｅｓの場合）、そのライセンス鍵をフラッシュメモリ１４３から読み出し、暗号通信を利用して、当該指示の送信元であるオーディオ再生装置１８/ビデオ再生装置１９に送信する（Ｓ１００８）。

なお、Ｓ１００４において指示の送信元がオーディオ再生装置１８/ビデオ再生装置１９であることを認証できなかった場合、および、Ｓ１００６において所望のライセンス鍵がフラッシュメモリ１４３に格納されていなかった場合、鍵格納専用装置１４のＣＰＵ１４１は、ＣＰＵ１１にその旨伝える。これを受けて、ＣＰＵ１１は表示装置１７にエラー表示を行うなど、所定のエラー処理を行う（Ｓ１００７）。

さて、コンテンツデータ再生のためのライセンス鍵送信指示を送信したオーディオ再生装置１８/ビデオ再生装置１９の暗複号化回路１８１/１９１は、鍵格納専用装置１４からライセンス鍵を受け取ると、コンテンツ格納装置１３から再生対象の暗号化されたコンテンツデータを読み出す（Ｓ１００９）。そして、これをライセンス鍵で復号して、デコーダ回路１８２/１９２に渡す。デコーダ回路１８２/１９２は、暗復号化回路１８１/１９１から受け取ったコンテンツデータを必要に応じて伸長し、再生してオーディオ/ビデオデータを得、ステレオ/モニタに出力する（Ｓ１０１０）。

次に、図６に示すフローにおける鍵格納専用装置１４およびオーディオ再生装置１８/ビデオ再生装置１９間のデータのやり取りについて、その一例を説明する。

図７は、図６に示すフローにおける鍵格納専用装置１４およびオーディオ再生装置１８/ビデオ再生装置１９間のデータのやり取りの一例を説明するためのシーケンス図である。

オーディオ再生装置１８/ビデオ再生装置１９の暗復号化回路１８１/１９１は、図６のＳ１００２において、自身の認証データと、再生対象の暗号化されたコンテンツデータの識別情報と、予め保持しているメディアクラス秘密鍵K_{PMC}と対のメディアクラス公開鍵K_{OMC}とを含んだライセンス鍵送信指示を作成し、これを鍵格納専用装置１４に送信する（Ｔ１００１）。

これを受けて、鍵格納専用装置１４のＣＰＵ１４１は、図６のＳ１００４～Ｓ１００７において、オーディオ再生装置１８/ビデオ再生装置１９の認証、および、フラッシュメモリ１４３に要求されたライセンス鍵が格納されていることの確認を行う（Ｔ１００２）。それから、ＣＰＵ１４１は、セッション鍵K_{S1}を生成し（Ｔ１００３）、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵K_{OMC}で暗号化して、当該指示の送信元であるオーディオ再生装置１８/ビデオ再生装置１９に送信する（Ｔ１００４）。

これを受けて、オーディオ再生装置１８/ビデオ再生装置１９の暗複号化回路１８１/１９１は、暗号化されたセッション鍵K_{S1}を予め保持しているメディアクラス秘密鍵K_{PMC}で復号し、セッション鍵K_{S1}を得る（Ｔ１００５）。それから、乱数K_{S2}を生成し（Ｔ１００６）、セッション鍵K_{S1}で暗号化して、鍵格納専用装置１４に送信する（Ｔ１００７）。

これを受けて、鍵格納専用装置１４のＣＰＵ１４１は、暗号化された乱数K_{S2}を、セッション鍵K_{S1}で復号し、乱数K_{S2}を得る（Ｔ１００８）。そして、送信を要求されているライセンス鍵K_Cを乱数K_{S2}で暗号化して、ライセンス鍵送信指示の送信元であるオーディオ再生装置１８/ビデオ再生装置１９に送信する（Ｔ１００９）。

これを受けて、オーディオ再生装置１８/ビデオ再生装置１９の暗複

号化回路１８１/１９１は、暗号化されたライセンス鍵K_cを乱数K_{s2}を用いて復号し、ライセンス鍵K_cを得る（Ｔ１０１０）。

以上、コンテンツデータを再生する場合の動作について説明した。

次に、メモリカード３０からライセンス鍵を入手する場合の動作について説明する。

図８は、本実施形態が適用されたコンテンツ再生装置に接続されたメモリカード３０からライセンス鍵を入手する場合の動作を説明するためのフロー図である。このフローは、たとえば、本コンテンツ再生装置にメモリカード３０が装着された状態で、ユーザが入力装置１６を用いて、表示装置１７に表示された、メモリカード３０に格納されているライセンス鍵に対応するコンテンツ名称のリストのなかから、入手対象のライセンス鍵に対応するコンテンツを選択し、ライセンス鍵入手指示を入力すると開始される。

まず、ＣＰＵ１１は、入力装置１６を介してユーザよりライセンス鍵入手指示を受け付けたならば、その旨を鍵格納専用装置１４に送信する（Ｓ２００１）。

ＣＰＵ１１よりライセンス鍵入手指示を受け取った鍵格納専用装置１４のＣＰＵ１４１は、自身の認証データと入手対象のライセンス鍵の識別情報（たとえば当該鍵で復号可能なコンテンツの名称）を含んだ、当該ライセンス鍵入手のためのライセンス鍵送信指示を、カード接続装置２０に接続されたメモリカード３０に送信する（Ｓ２００２）。

メモリカード３０のＣＰＵは、ライセンス鍵入手のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う（Ｓ２００３）。たとえば、認証データが予め本メモリカード３０に登録されている鍵格納専用装置であることを示しているか否かを調べる。そして、当該指示の送信元が鍵格納専用装置１４であるこ

とを認証したならば（Ｓ２００４でＹｅｓの場合）、当該指示に含まれる識別情報により特定されるライセンス鍵がメモリカード３０内に格納されているか否かを調べる（Ｓ２００５）。格納されていれば（Ｓ２００６でＹｅｓの場合）、そのライセンス鍵を読み出し、暗号通信を利用して、当該指示の送信元である鍵格納専用装置１４に送信する（Ｓ２００８）。それから、送信したライセンス鍵をメモリカード３０内から消去する（Ｓ２００９）。

なお、Ｓ２００４において指示の送信元が鍵格納専用装置１４であることを認証できなかった場合、および、Ｓ２００６において所望のライセンス鍵がメモリカード３０内に格納されていなかった場合、メモリカード３０のＣＰＵは、ＣＰＵ１１にその旨伝える。これを受けて、ＣＰＵ１１は表示装置１７にエラー表示を行うなど、所定のエラー処理を行う（Ｓ２００７）。

さて、ライセンス鍵入手のためのライセンス鍵送信指示を送信した鍵格納専用装置１４のＣＰＵ１４１は、カード接続装置２０に接続されたメモリカード３０からライセンス鍵を受け取ると、これをたとえば当該鍵で復号可能なコンテンツデータのコンテンツ名称に対応付けてフラッシュメモリ１４３に格納する（Ｓ２０１０）。

次に、図８に示すフローにおける鍵格納専用装置１４およびメモリカード３０間のデータのやり取りについて、その一例を説明する。

図９は、図８に示すフローにおける鍵格納専用装置１４およびメモリカード３０間のデータのやり取りの一例を説明するためのシーケンス図である。

鍵格納専用装置１４のＣＰＵ１４１は、図８のＳ２００２において、自身の認証データと、入手対象のライセンス鍵の識別情報と、予め保持しているメディアクラス秘密鍵K'_{PMC}と対のメディアクラス公開鍵K'_{0}

$_{MC}$とを含んだライセンス鍵送信指示を作成し、これをメモリカード３０に送信する（Ｔ２００１）。

これを受けて、メモリカード３０のＣＰＵは、図８のＳ２００４～Ｓ２００７において、鍵格納専用装置１４の認証、および、メモリカード３０内に要求されたライセンス鍵が格納されていることの確認を行う（Ｔ２００２）。それから、メモリカード３０のＣＰＵは、セッション鍵K_{S1}を生成し（Ｔ２００３）、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵K'_{OMC}で暗号化して、当該指示の送信元である鍵格納専用装置１４に送信する（Ｔ２００４）。

これを受けて、鍵格納専用装置１４のＣＰＵ１４１は、暗号化されたセッション鍵K_{S1}を予め保持しているメディアクラス秘密鍵K'_{PMC}で復号し、セッション鍵K_{S1}を得る（Ｔ２００５）。それから、乱数K_{S2}を生成し（Ｔ２００６）、これと、予め保持しているメディア固有秘密鍵K'_{PM}と対のメディア固有公開鍵K'_{OM}とを、セッション鍵K_{S1}で暗号化して、メモリカード３０に送信する（Ｔ２００７）。

これを受けて、メモリカード３０のＣＰＵは、暗号化された乱数K_{S2}とメディア固有公開鍵K'_{OM}を、セッション鍵K_{S1}で復号し、乱数K_{S2}とメディア固有公開鍵K'_{OM}を得る（Ｔ２００８）。そして、送信を要求されているライセンス鍵K_Cをメディア固有公開鍵K'_{OMC}で暗号化し、さらにこれを乱数K'_{S2}で暗号化して、ライセンス鍵送信指示の送信元である鍵格納専用装置１４に送信する（Ｔ２００９）。

これを受けて、鍵格納専用装置１４のＣＰＵ１４１は、暗号化されたライセンス鍵K_Cを乱数K_{S2}とメディア固有秘密鍵K'_{PM}を用いて復号し、ライセンス鍵K_Cを得る（Ｔ２０１０）。

以上、メモリカード３０からライセンス鍵を入手する場合の動作について説明した。

次に、本コンテンツ再生装置の鍵格納専用装置１４に格納されているライセンス鍵をメモリカード３０へ移動する場合の動作について説明する。

図１０は、本実施形態が適用されたコンテンツ再生装置の鍵格納専用装置１４から本コンテンツ再生装置に接続されたメモリカード３０へライセンス鍵を移動する場合の動作を説明するためのフロー図である。このフローは、たとえば、本コンテンツ再生装置にメモリカード３０が装着された状態で、ユーザが入力装置１６を用いて、表示装置１７に表示された、鍵格納専用装置１４に格納されているライセンス鍵に対応するコンテンツ名称のリストのなかから、移動対象のライセンス鍵に対応するコンテンツを選択し、ライセンス鍵移動指示を入力すると開始される。

まず、ＣＰＵ１１は、入力装置１６を介してユーザよりライセンス鍵移動指示を受け付けたならば、その旨をメモリカード３０に送信する（Ｓ３００１）。

ＣＰＵ１１よりライセンス鍵移動指示を受け取ったメモリカード３０のＣＰＵは、自身の認証データと移動対象のライセンス鍵の識別情報（たとえば当該鍵で復号可能なコンテンツの名称）を含んだ、当該ライセンス鍵移動のためのライセンス鍵送信指示を、鍵格納専用装置１４に送信する（Ｓ３００２）。

鍵格納専用装置１４のＣＰＵ１４１は、ライセンス鍵移動のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う（Ｓ３００３）。たとえば、認証データが予め本鍵格納専用装置１４に登録されているメモリカード３０であることを示しているか否かを調べる。そして、当該指示の送信元がメモリカード３０であることを認証したならば（Ｓ３００４でＹｅｓの場合）、当該指示に含まれる識別情報により特定されるライセンス鍵がフラッシュメモ

リ１４３内に格納されているか否かを調べる（Ｓ３００５）。格納されていれば（Ｓ３００６でＹｅｓの場合）、そのライセンス鍵を読み出し、暗号通信を利用して、当該指示の送信元であるメモリカード３０に送信する（Ｓ３００８）。それから、送信したライセンス鍵をフラッシュメモリ１４３内から消去する（Ｓ３００９）。

なお、Ｓ３００４において指示の送信元がメモリカード３０であることを認証できなかった場合、および、Ｓ３００６において所望のライセンス鍵がフラッシュメモリ１４３内に格納されていなかった場合、鍵格納専用装置１４のＣＰＵ１４１は、ＣＰＵ１１にその旨伝える。これを受けて、ＣＰＵ１１は表示装置１７にエラー表示を行うなど、所定のエラー処理を行う（Ｓ３００７）。

さて、ライセンス鍵移動のためのライセンス鍵送信指示を送信したメモリカード３０のＣＰＵは、鍵格納専用装置１４からライセンス鍵を受け取ると、これをたとえば当該鍵で復号可能なコンテンツデータのコンテンツ名称に対応付けてメモリカード３０内に格納する（Ｓ３０１０）。

なお、図１０に示すフローにおける鍵格納専用装置１４およびメモリカード３０間のデータのやり取りは、図９に示すシーケンス図において、鍵格納専用装置１４およびメモリカード３０の動作を互いに交換したものとなる。

以上、メモリカード３０へライセンス鍵を移動する場合の動作について説明した。

なお、通信装置１５に接続された携帯電話機/据置型電話機を利用して、オンラインシステムやインターネットなどのネットワークを介して、コンテンツ配信センタ（不図示）からライセンス鍵を入手する場合の動作は、一般的な、ネットワークを介したデータダウンロードと同じものでよい。ただし、正当な権利を有する者のみがライセンス鍵を入手でき

るようにするために、鍵格納専用装置１４とコンテンツ配信センタとの間で認証処理を行い、コンテンツ配信センタが鍵格納専用装置１４を認証した場合にのみ、ライセンス鍵のダウンロードを許可するようにすることが好ましい。また、コンテンツデータのコンテンツ格納装置１３へのダウンロードは、たとえば、メモリカード３０に格納されたコンテンツデータをコピーしてコンテンツ格納装置１３に格納するようにしてもよいし、あるいは、通信装置１５に接続された携帯電話機/据置型電話機を利用して、オンラインシステムやインターネットなどのネットワークを介して、コンテンツ配信センタ（不図示）から入手し、コンテンツ格納装置１３に格納するようにしてもよい。いずれにしても、コンテンツデータは暗号化されており、対応するライセンス鍵がなければ復号・再生できない。

以上、本発明の１実施形態について説明した。

本実施形態において、コンテンツ格納装置１３に格納されたコンテンツデータは暗号化されているので、対応するライセンス鍵がなければ復号し再生することができない。したがって、コンテンツ格納装置１３にコピー防止機能といった特別な機能を設ける必要がなくなるため、コンテンツ格納装置１３として、一般に市販されている大容量のハードディスク装置などを利用できる。このため、大量のコンテンツデータを格納することが可能となる。

また、コンテンツ格納装置１３に格納されたコンテンツデータを復号するためには対応するライセンス鍵が必要となるため、このライセンス鍵が鍵格納専用装置１４に格納されていなければ、当該コンテンツデータを再生することができない。したがって、正当な権利者（対応するライセンス鍵を有する者）のみに、コンテンツデータの再生を許可することができ、コンテンツ著作者などの保護を図ることができる。

さらに、本実施形態では、暗号化されたコンテンツデータの復号を、コンテンツデータの再生を行うオーディオ再生装置１８/ビデオ再生装置１９で行うようにしている。そして、鍵格納専用装置１４は、ライセンス鍵の送信相手がオーディオ再生装置１８/ビデオ再生装置１であることを認証した場合に、当該ライセンス鍵を暗号通信を利用してオーディオ再生装置１８/ビデオ再生装置１９に送るようにしている。このようにすることで、ライセンス鍵が外部に漏れる可能性をより低くすることができ、セキュリティを向上できる。

くわえて、本実施形態において、鍵格納専用装置１４は、ライセンス鍵の送信相手がメモリカード３０である場合、送信したライセンス鍵を鍵格納専用装置１４の記憶内容から消去するようにしている。つまり、鍵格納専用装置１４にライセンス鍵のコピー防止機能を設けている。このようにすることで、ライセンス鍵が不正にコピーされる可能性を減らすことができる。

なお、一般に、鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば、著しく小さい。このため、鍵格納専用装置１４の記憶部をフラッシュメモリ１４３で構成した場合でも、当該フラッシュメモリ１４３に多くのライセンス鍵を格納することができる。したがって、家のなかでコンテンツデータの再生を楽しむような据置型に適したコンテンツ再生装置を提供できる。

なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

たとえば、上記の実施形態では、暗号化されたコンテンツデータがたとえばハードディスク装置などの記憶装置でなるコンテンツ格納装置１３に格納されている場合を例に取り説明した。しかしながら、本発明はこれに限定されるものではない。暗号化されたコンテンツデータは、D

ＶＤやＣＤなどの可搬性を有する記憶媒体に格納された形態で提供されるものでもよい。この場合、本実施形態において、コンテンツ格納装置１３に代えて前記可搬性を有する記憶媒体から暗号化されたコンテンツデータを読み取る読取装置を設けるようにすればよい。

また、上記の実施形態において、鍵格納専用装置１４を装着自在に構成してもよい。たとえば、鍵格納専用装置１４として、メモリカード３０を用い、カード接続装置２０に装着するようにしてもよい。あるいは、本コンテンツ再生装置に、鍵格納専用装置１４専用のスロットを設け、このスロットに鍵格納専用装置１４を装着するようにしてもよい。上述したように、鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば著しく小さいので、多くのライセンス鍵を鍵格納専用装置１４に格納することができる。このため、再生するコンテンツを変えるときに鍵格納専用装置１４を差し替えなければならないといった事態が頻繁に生じるのを防ぐことができる。したがって、家のなかでコンテンツデータの再生を楽しむような据置型に適したコンテンツ再生装置を提供できる。

さらに、上記の実施形態では、ライセンス鍵を暗号化されたコンテンツデータ毎に用意しているが、本発明はこれに限定されない。たとえば、複数の暗号化されたコンテンツデータを１グループとして、グループ毎に、当該グループに属する暗号化されたコンテンツデータを復号するためのライセンス鍵を用意するようにしてもよい。

以上説明したように、本発明によれば、コンテンツ著作者などの保護を図りつつも、メモリカードの交換なしに、大量のコンテンツデータを再生できるようにすることが可能となる。

請求の範囲

1．暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータを格納するコンテンツ格納手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、前記コンテンツ格納手段とは別個に設けられた計算機能付き鍵格納手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記計算機能付き鍵格納手段は、

通信相手を認証する認証手段を有し、前記認証手段により前記再生手段が通信相手として認証された場合に、暗号通信を利用して、前記再生手段に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

前記再生手段は、

前記コンテンツ格納手段から読み出された、再生対象の暗号化されたコンテンツデータを、前記計算機能付き鍵格納手段より暗号通信を利用して送信された鍵を用いて復号し、再生すること

を特徴とするコンテンツ再生装置。

2．請求項1記載のコンテンツ再生装置であって、

前記計算機能付き鍵格納手段は、本コンテンツ再生装置に装着自在に構成されていること

を特徴とするコンテンツ再生装置。

3．請求項1記載のコンテンツ再生装置であって、

暗号化されたコンテンツデータを復号するための鍵が記憶された計算機能付き記憶媒体を接続するための接続手段をさらに有し、

前記計算機能付き鍵格納手段は、

前記接続手段に接続された前記計算機能付き記憶媒体より、暗号通信を利用して送信された鍵を格納すること

を特徴とするコンテンツ再生装置。

4．請求項3記載のコンテンツ再生装置であって、

前記計算機能付き鍵格納手段は、

前記認証手段により、前記接続手段に接続された前記計算機能付き記憶媒体が通信相手として認証された場合に、暗号通信を利用して、自身が保持している鍵を読み出して前記計算機能付き記憶媒体に送信するとともに、送信した鍵を記憶内容から消去すること

を特徴とするコンテンツ再生装置。

5．暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータが記憶された可搬性を有する記憶媒体から、再生対象の暗号化されたコンテンツデータを読み取るコンテンツ読取手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、計算機能付き鍵格納手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記計算機能付き鍵格納手段は、

通信相手を認証する認証手段を有し、前記認証手段により前記再生手段が通信相手として認証された場合に、暗号通信を利用して、前記再生手段に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

前記再生手段は、

前記コンテンツ読取手段を介して前記記憶媒体から読み出された、再生対象の暗号化されたコンテンツデータを、前記計算機能付き鍵格納手段より暗号通信を利用して送信された鍵を用いて復号し、再生すること

を特徴とするコンテンツ再生装置。

6．請求項5記載のコンテンツ再生装置であって、

前記計算機能付き鍵格納手段は、本コンテンツ再生装置に装着自在に構成されていること

を特徴とするコンテンツ再生装置。

7．請求項5記載のコンテンツ再生装置であって、

暗号化されたコンテンツデータを復号するための鍵が記憶された計算機能付き記憶媒体を接続するための接続手段をさらに有し、

前記計算機能付き鍵格納手段は、

前記接続手段に接続された前記計算機能付き記憶媒体より、暗号通信を利用して送信された鍵を格納すること

を特徴とするコンテンツ再生装置。

8．請求項7記載のコンテンツ再生装置であって、

前記計算機能付き鍵格納手段は、

前記認証手段により、前記接続手段に接続された前記計算機能付き記憶媒体が通信相手として認証された場合に、暗号通信を利用して、自身が保持している鍵を読み出して前記計算機能付き記憶媒体に送信するとともに、送信した鍵を記憶内容から消去すること

を特徴とするコンテンツ再生装置。

9．暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータを格納するコンテンツ格納手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、計算機能付き鍵格納装置を接続するための接続手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記再生手段は、

前記コンテンツ格納手段から読み出された、再生対象の暗号化されたコンテンツデータを、前記接続手段によって接続された前記計算機能付き鍵格納装置より、暗号通信を利用して送信された鍵を用いて復号し、再生すること

を特徴とするコンテンツ再生装置。

10．暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータが記憶された可搬性を有する記憶媒体から、再生対象の暗号化されたコンテンツデータを読み取るコンテンツ読取手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、計算機能付き鍵格納装置を接続するための接続手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記再生手段は、

前記コンテンツ読取手段を介して前記記憶媒体から読み出された、再生対象の暗号化されたコンテンツデータを、前記接続手段によって接続された前記計算機能付き鍵格納装置より、暗号通信を利用して送信された鍵を用いて復号し、再生すること

を特徴とするコンテンツ再生装置。

１１．暗号化されたコンテンツデータを復号して再生するコンテンツ再生装置に装着されて用いられる計算機能付き鍵格納装置であって、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する鍵格納手段と、

通信相手を認証する認証手段と、

前記認証手段により前記コンテンツ再生装置が通信相手として認証された場合に、再生対象の暗号化されたコンテンツデータに対応する鍵を前記鍵格納手段から読み出し、暗号通信を利用して前記コンテンツ再生装置に送信する通信手段と、を有すること

を特徴とする計算機能付き鍵格納装置。

１２．暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータを格納するコンテンツ格納手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータの復号するための鍵を格納する、前記コンテンツ格納手段とは別個に設けられた復号鍵を記録する鍵格納手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記復号鍵を記録する鍵格納手段は、

通信相手を認証する認証手段を有し、前記認証手段により前記再生手段が通信相手として認証された場合に、暗号通信を利用して、前記再生手段に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

前記再生手段は、

前記コンテンツ格納手段から読み出された、再生対象の暗号化されたコンテンツデータを、前記復号鍵を記録する鍵格納手段より暗号通信を利用して送信された鍵を用いて復号し、再生すること

を特徴とするコンテンツ再生装置。

図1

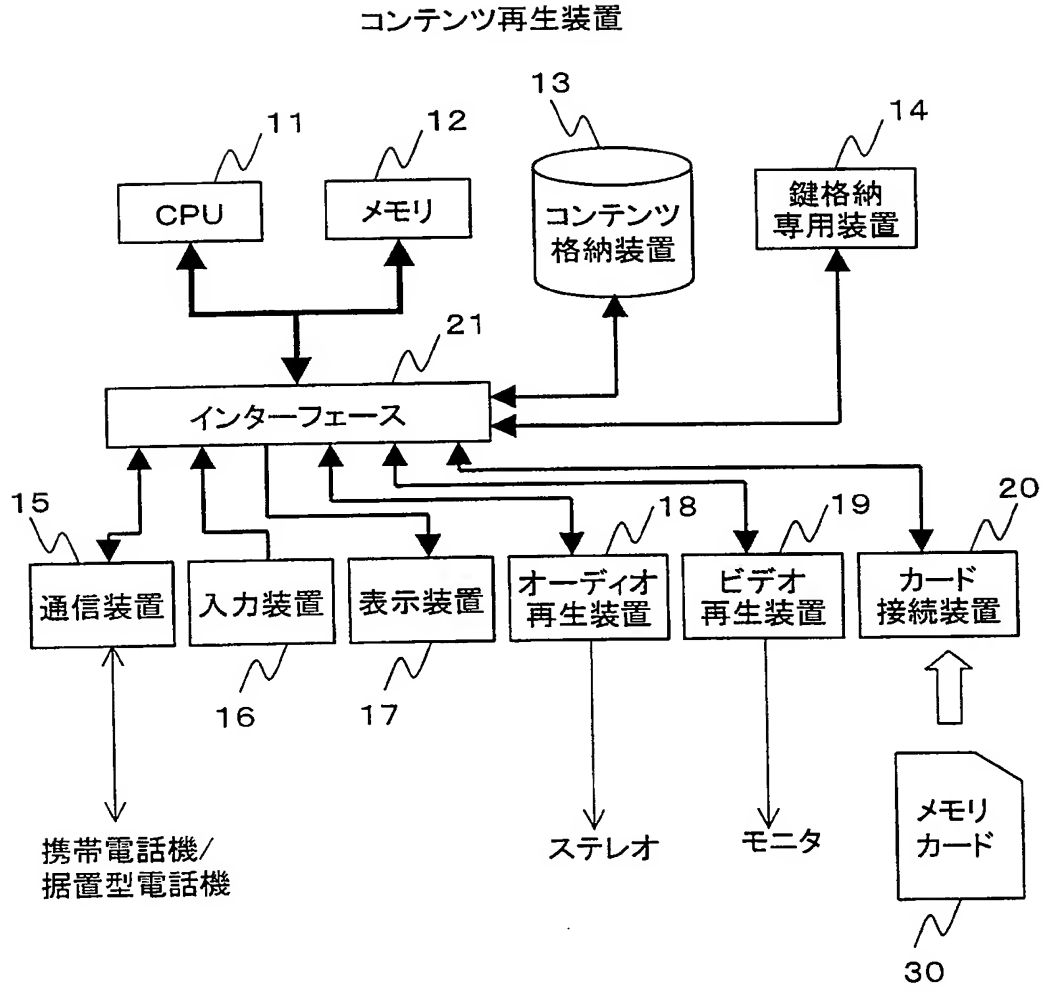

コンテンツ再生装置
11
12
13
14
CPU
メモリ
コンテンツ格納装置
鍵格納専用装置
21
インターフェース
15
18
19
20
通信装置
入力装置
表示装置
オーディオ再生装置
ビデオ再生装置
カード接続装置
16
17
携帯電話機/据置型電話機
ステレオ
モニタ
メモリカード
30

図2

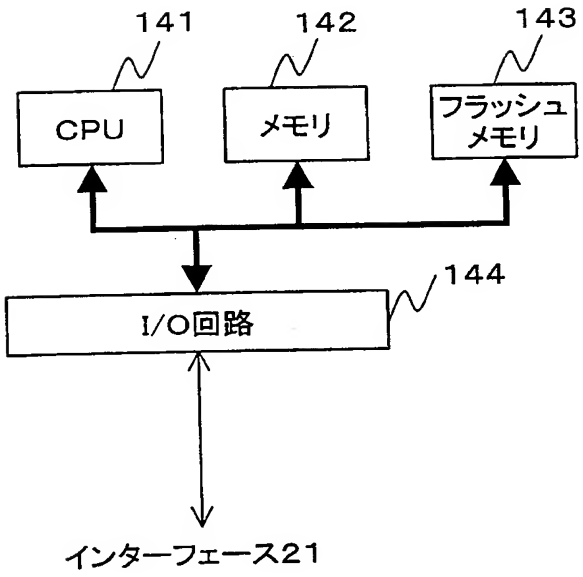


図3

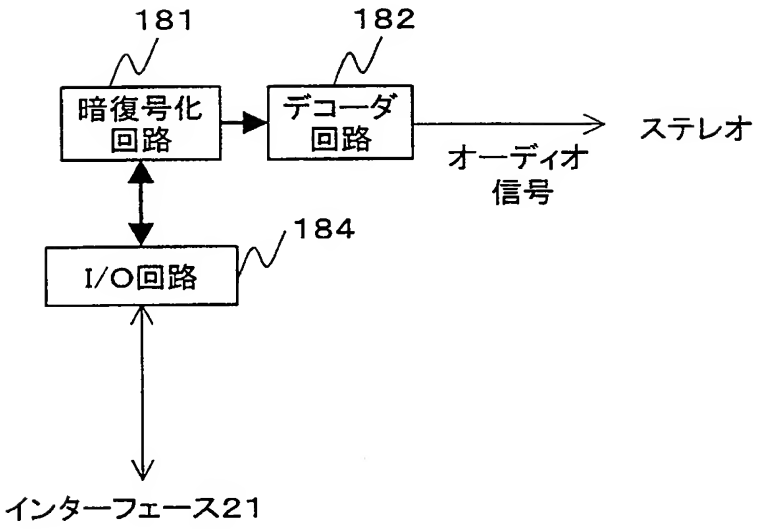

オーディオ再生装置18
181
182
暗復号化回路
デコーダ回路
ステレオ
オーディオ信号
184
I/O回路
インターフェース21

図4

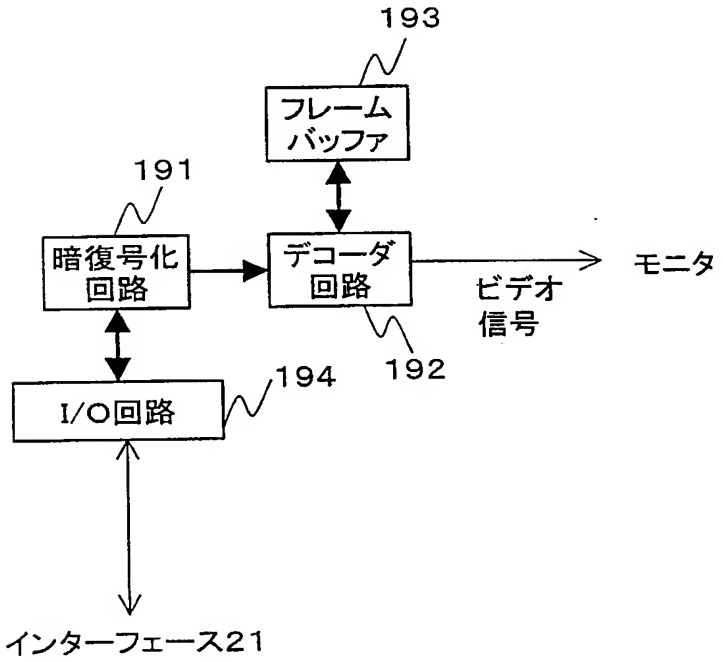

ビデオ再生装置19
193
フレーム
バッファ
191
暗復号化
回路
デコーダ
回路
モニタ
ビデオ
信号
192
194
I/O回路
インターフェース21

図5

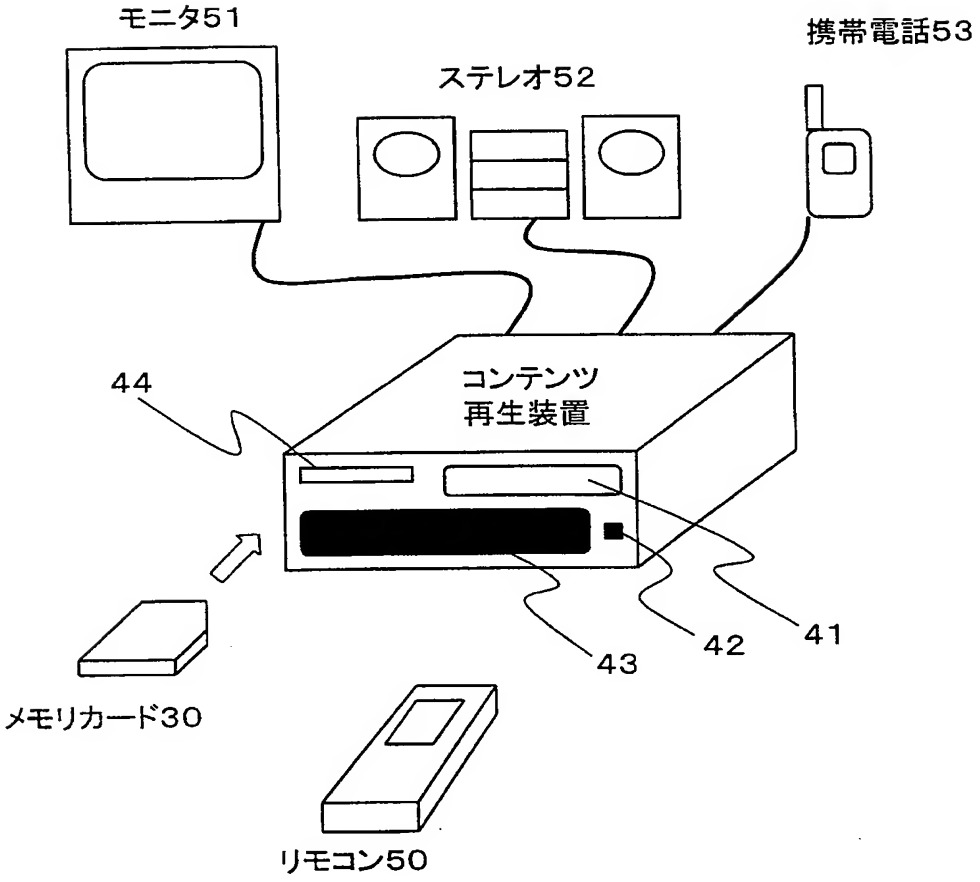


図6

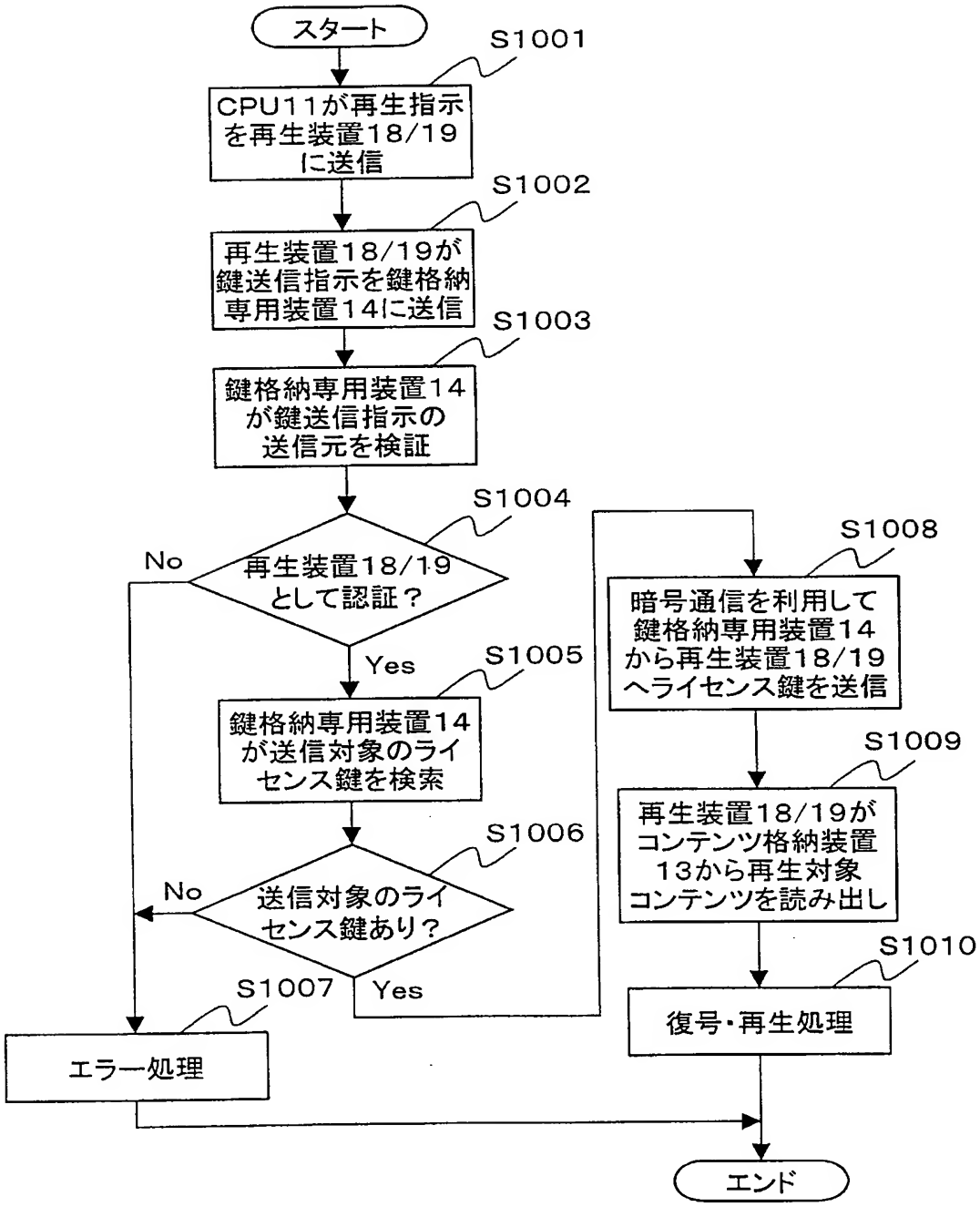
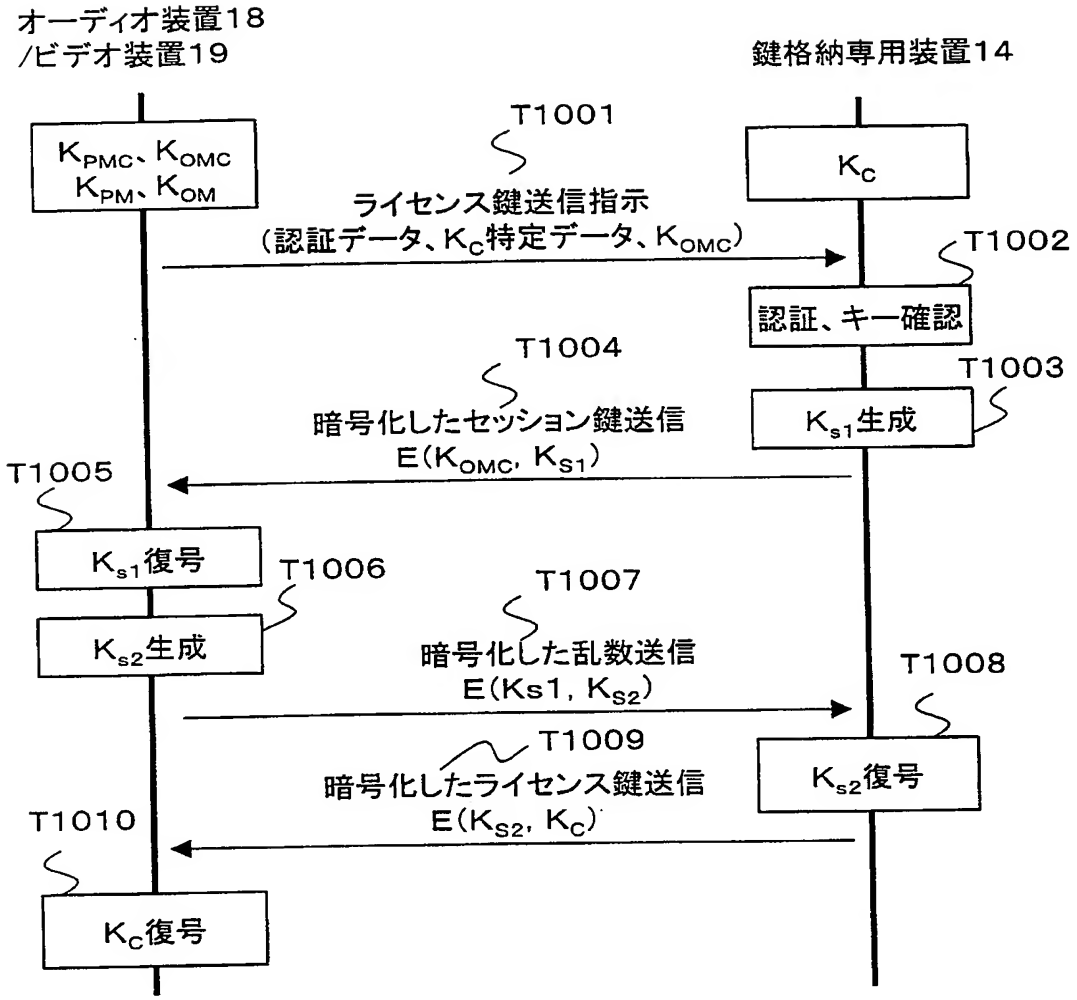

スタート
S1001
CPU11が再生指示を再生装置18/19に送信
S1002
再生装置18/19が鍵送信指示を鍵格納専用装置14に送信
S1003
鍵格納専用装置14が鍵送信指示の送信元を検証
S1004
再生装置18/19として認証？
No
Yes
S1005
鍵格納専用装置14が送信対象のライセンス鍵を検索
S1006
送信対象のライセンス鍵あり？
No
Yes
S1007
エラー処理
S1008
暗号通信を利用して鍵格納専用装置14から再生装置18/19へライセンス鍵を送信
S1009
再生装置18/19がコンテンツ格納装置13から再生対象コンテンツを読み出し
S1010
復号・再生処理
エンド

図7



K_{PMC}:メディアクラス秘密鍵
K_{OMC}:メディアクラス公開鍵
K_{S2} :乱数

K_C:ライセンス鍵
K_{s1}:セッション鍵

図8

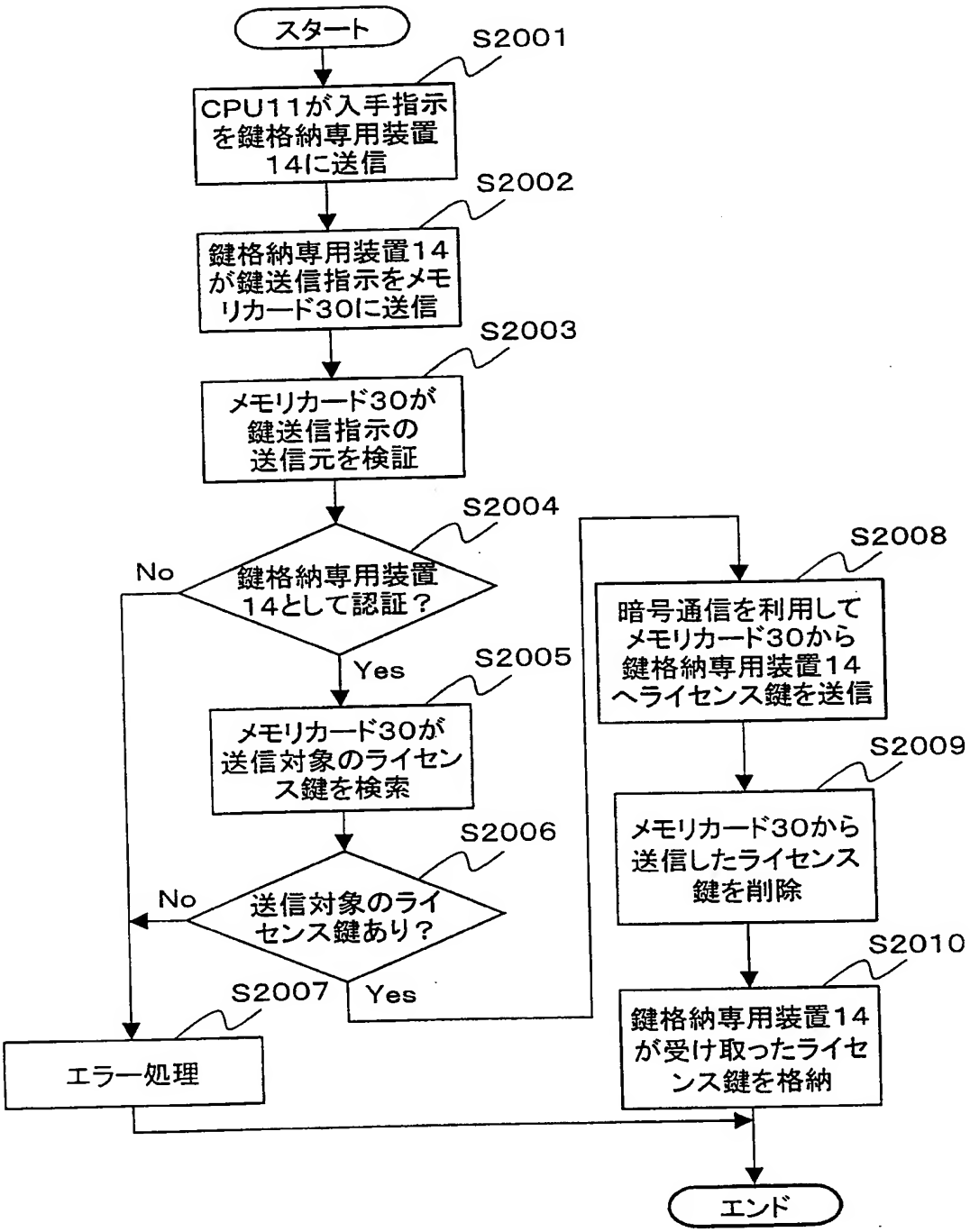
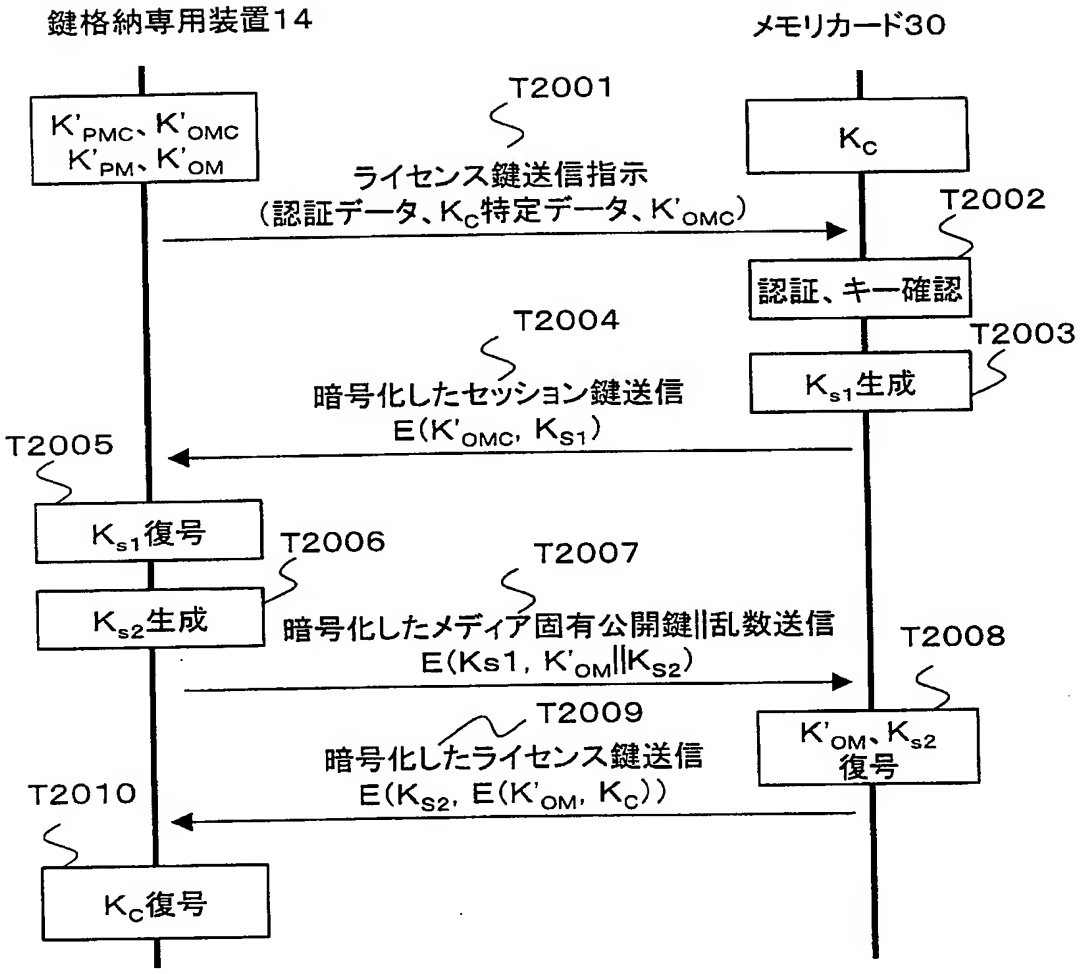

スタート
S2001
CPU11が入手指示を鍵格納専用装置14に送信
S2002
鍵格納専用装置14が鍵送信指示をメモリカード30に送信
S2003
メモリカード30が鍵送信指示の送信元を検証
S2004
鍵格納専用装置14として認証？
No
Yes
S2005
メモリカード30が送信対象のライセンス鍵を検索
S2006
送信対象のライセンス鍵あり？
No
Yes
S2007
エラー処理
S2008
暗号通信を利用してメモリカード30から鍵格納専用装置14へライセンス鍵を送信
S2009
メモリカード30から送信したライセンス鍵を削除
S2010
鍵格納専用装置14が受け取ったライセンス鍵を格納
エンド

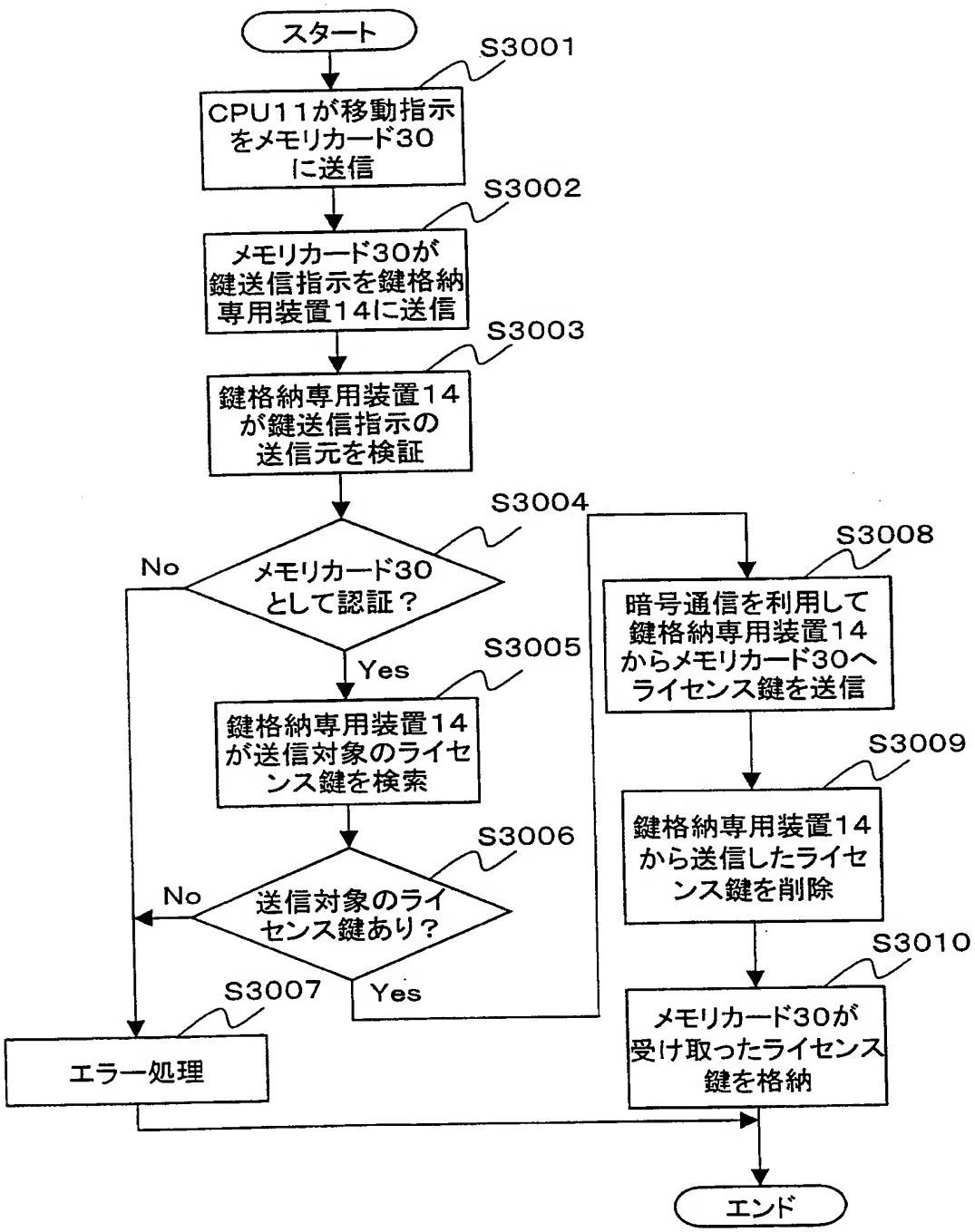
図9



K'PMC:メディアクラス秘密鍵
K'OMC:メディアクラス公開鍵
K'PM :メディア固有秘密鍵
K'OM :メディア固有公開鍵
KS2 :乱数

Kc:ライセンス鍵
Ks1:セッション鍵

図10


スタート
S3001
CPU11が移動指示をメモリカード30に送信
S3002
メモリカード30が鍵送信指示を鍵格納専用装置14に送信
S3003
鍵格納専用装置14が鍵送信指示の送信元を検証
S3004
メモリカード30として認証？
No
Yes
S3005
鍵格納専用装置14が送信対象のライセンス鍵を検索
S3006
送信対象のライセンス鍵あり？
No
Yes
S3007
エラー処理
S3008
暗号通信を利用して鍵格納専用装置14からメモリカード30へライセンス鍵を送信
S3009
鍵格納専用装置14から送信したライセンス鍵を削除
S3010
メモリカード30が受け取ったライセンス鍵を格納
エンド

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/02003

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L9/10, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L9/10, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Kiyoshi YAMANAKA et al., "Multimedia on demande Service ni okeru Joho Hogo System", NTT R & D, Vol.44, No.9, 10 September, 1995 (10.09.95) pp.813-818 pp.813-818	1-7,9-12 8
Y	JP, 9-307543, A (Matsushita Electric Ind. Co., Ltd.), 28 November, 1997 (28.11.97), Par. Nos. [0018] to [0019], [0022], [0024] to [0025]; Figs. 1 to 8 (Family: none)	8
A	"Kogata Memory Card de Ongaku Chosakuken wo mamoru", Nikkei Elecrtonics, 1999 3-22, No.739, 22 March, 1999 (22.03.99) pp.49-53	1-12
A	JP, 4-102185, A (NTT Data Tsushin K.K.), 03 April, 1992 (03.04.92), Full text; Figs. 1 to 2 (Family: none)	1-12

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 June, 2001 (08.06.01)	19 June, 2001 (19.06.01)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/02003

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 10-40172, A (Toshiba Corporation), 13 February, 1998 (13.02.98), Full text; Figs. 1 to 4 (Family: none)	1-12

国際調査報告

国際出願番号 PCT/JP01/02003

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9/08, H04L9/10, H04L9/32

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9/08, H04L9/10, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	山中喜義、高嶋洋一、小柳津育郎；“マルチメディアオンデマンドサービスにおける情報保護システム” NTT R&D, Vol. 44, No. 9, 10. 9月. 1995（10. 09. 95） pp. 813－818 pp. 813－818	1-7, 9-12 8
Y	JP, 9－307543, A（松下電器産業株式会社） 28. 11月. 1997（28. 11. 97） 第【0018】－【0019】段落、第【0022】段落、	8

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 08. 06, 01	国際調査報告の発送日 19.06.01
国際調査機関の名称及びあて先 日本国特許庁（ISA/JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 青木 重徳 印 5M 4229 電話番号 03－3581－1101 内線 3597

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	第【００２４】－【００２５】段落、図１－８ （ファミリーなし）	
A	“小型メモリ・カードで音楽著作権を守る” 日経エレクトロニクス，１９９９　３－２２，Ｎｏ．７３９， ２２．３月．１９９９（２２．０３．９９） ｐ．４９－５３	１－１２
A	ＪＰ，４－１０２１８５，Ａ（エヌ・ティ・ティ・データ通信株式会社） ３．４月．１９９２（０３．０４．９２） 全文，第１－２図 （ファミリーなし）	１－１２
A	ＪＰ，１０－４０１７２，Ａ（株式会社東芝） １３．２月．１９９８（１３．０２．９８） 全文，図１－４ （ファミリーなし）	１－１２